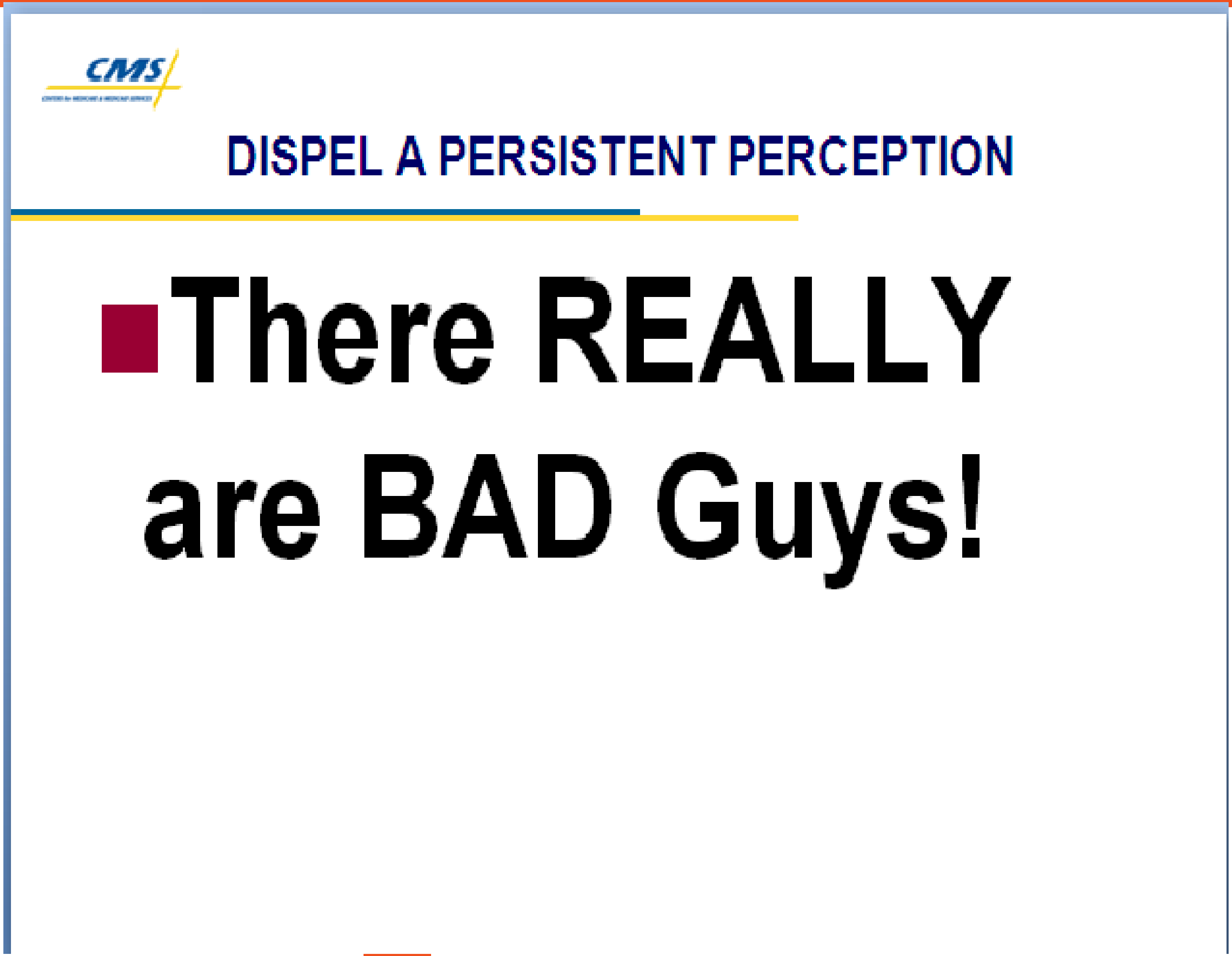
Authentication for Health Information Exchange

Anna Slomovic

Chief Privacy Officer, Anakam, Inc.

September 2010

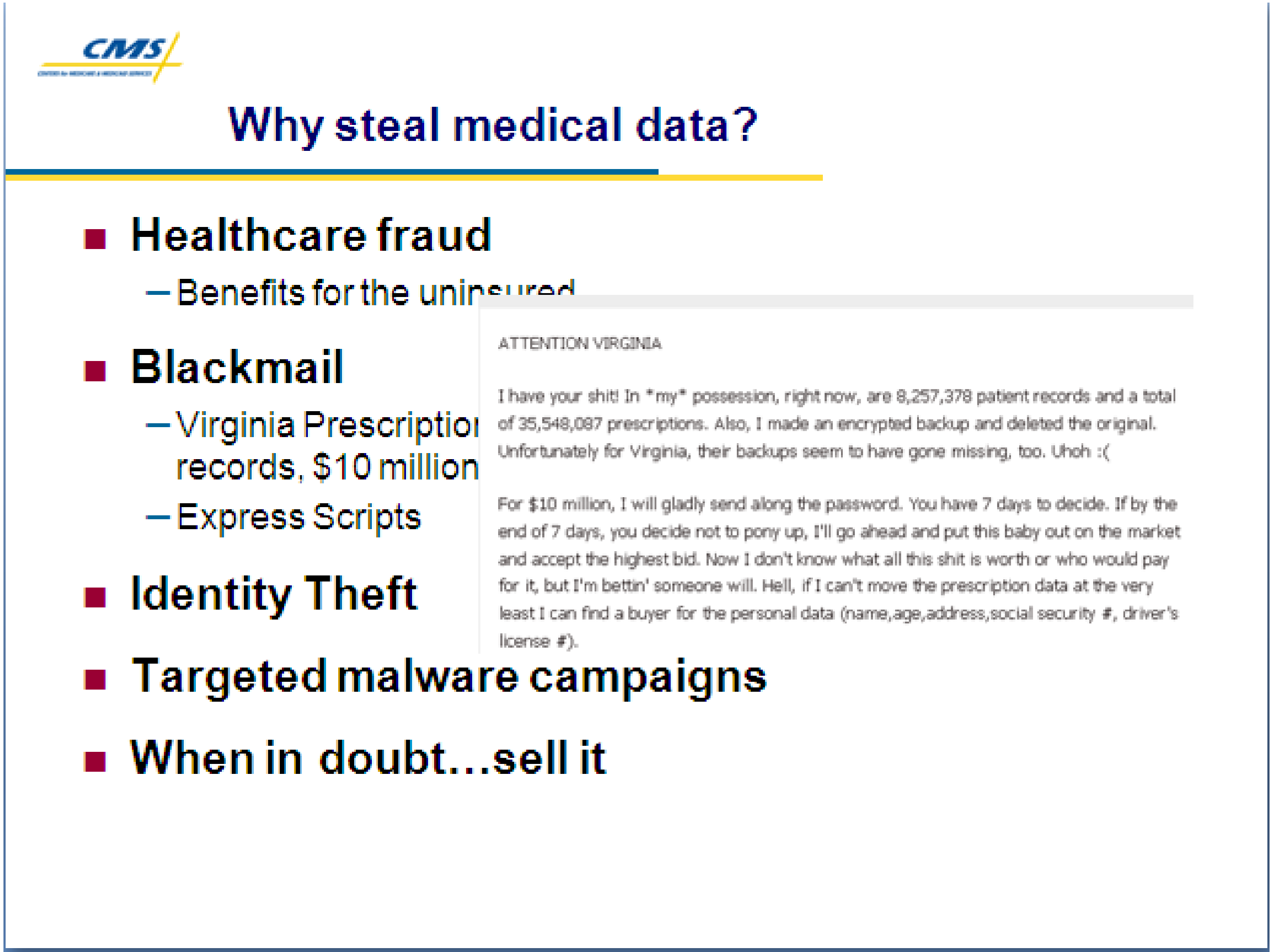
From Julie Boughn, CMS CIO



CMS

DISPEL A PERSISTENT PERCEPTION

- There REALLY are BAD Guys!



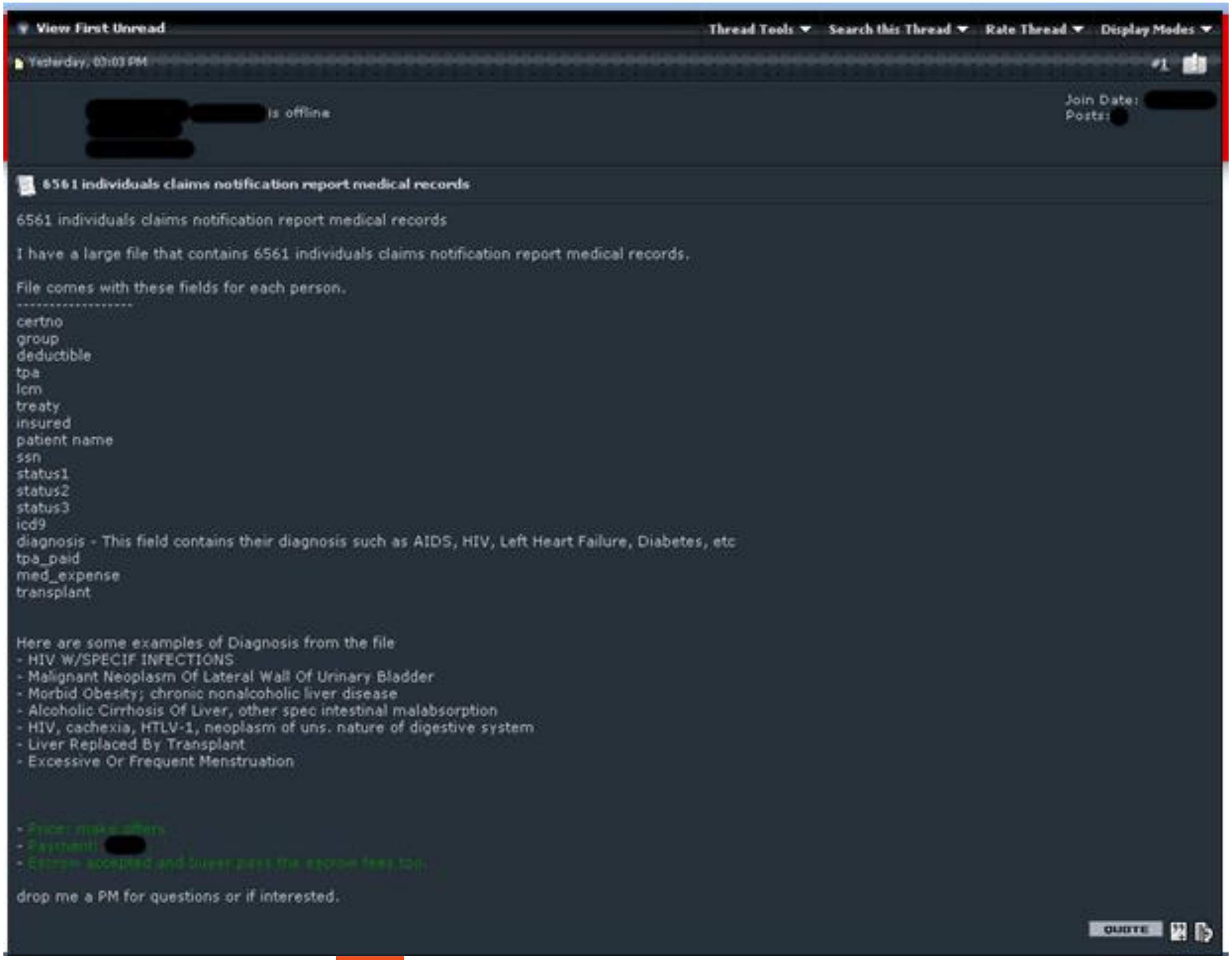
Why steal medical data?

- Healthcare fraud
  - Benefits for the uninsured
- Blackmail
  - Virginia Prescriptio
    records, $10 million
  - Express Scripts
- Identity Theft
- Targeted malware campaigns
- When in doubt…sell it

ATTENTION VIRGINIA

I have your shit! In *my* possession, right now, are 8,257,378 patient records and a total of 35,548,087 prescriptions. Also, I made an encrypted backup and deleted the original. Unfortunately for Virginia, their backups seem to have gone missing, too. Uhoh :(

For $10 million, I will gladly send along the password. You have 7 days to decide. If by the end of 7 days, you decide not to pony up, I'll go ahead and put this baby out on the market and accept the highest bid. Now I don't know what all this shit is worth or who would pay for it, but I'm bettin' someone will. Hell, if I can't move the prescription data at the very least I can find a buyer for the personal data (name,age,address,social security #, driver's license #).



Yesterday, 03:03 PM

[redacted] is offline

Join Date: [redacted]
Posts: [redacted]

6561 individuals claims notification report medical records

6561 individuals claims notification report medical records

I have a large file that contains 6561 individuals claims notification report medical records.

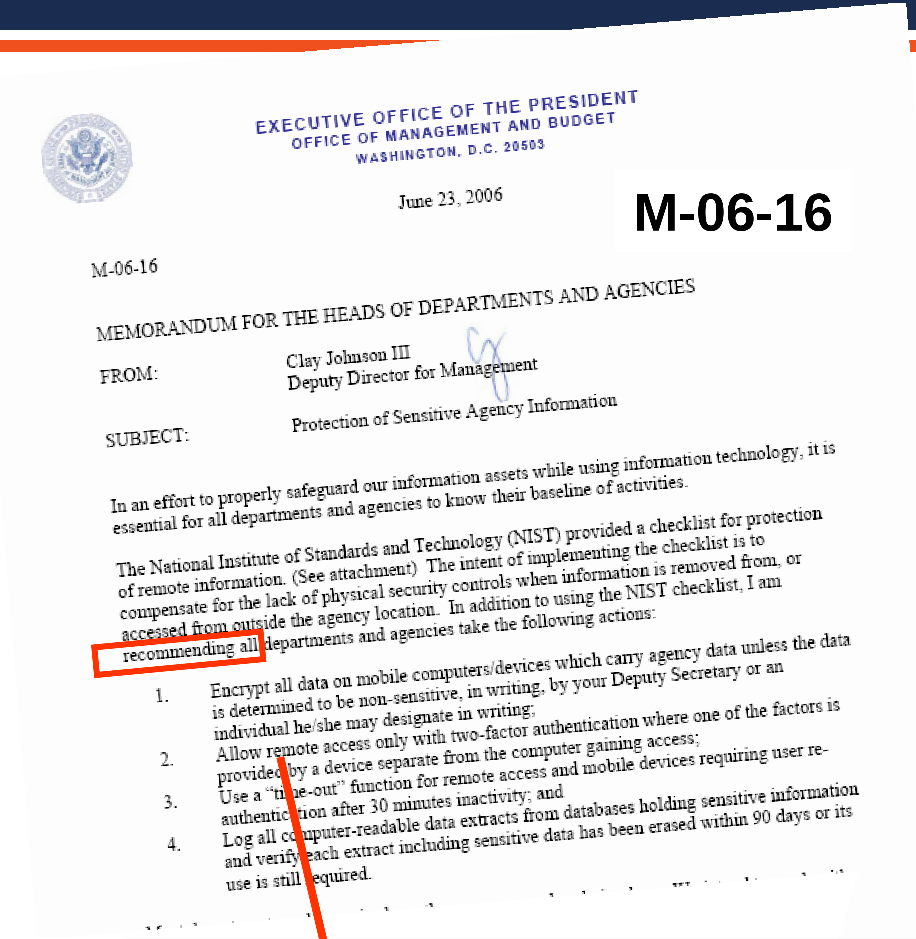
File comes with these fields for each person.
----
certno
group
deductible
tpa
lcm
treaty
insured
patient name
ssn
status1
status2
status3
icd9
diagnosis - This field contains their diagnosis such as AIDS, HIV, Left Heart Failure, Diabetes, etc
tpa_paid
med_expense
transplant

Here are some examples of Diagnosis from the file
- HIV W/SPECIF INFECTIONS
- Malignant Neoplasm Of Lateral Wall Of Urinary Bladder
- Morbid Obesity; chronic nonalcoholic liver disease
- Alcoholic Cirrhosis Of Liver, other spec intestinal malabsorption
- HIV, cachexia, HTLV-1, neoplasm of uns. nature of digestive system
- Liver Replaced By Transplant
- Excessive Or Frequent Menstruation

- Price: make offers
- Payment: [redacted]
- Escrow accepted and buyer pays the escrow fees too.

drop me a PM for questions or if interested.

Federal government requires two-factor authentication for access to PII



M-06-16

EXECUTIVE OFFICE OF THE PRESIDENT
OFFICE OF MANAGEMENT AND BUDGET
WASHINGTON, D.C. 20503

June 23, 2006

M-06-16

MEMORANDUM FOR THE HEADS OF DEPARTMENTS AND AGENCIES

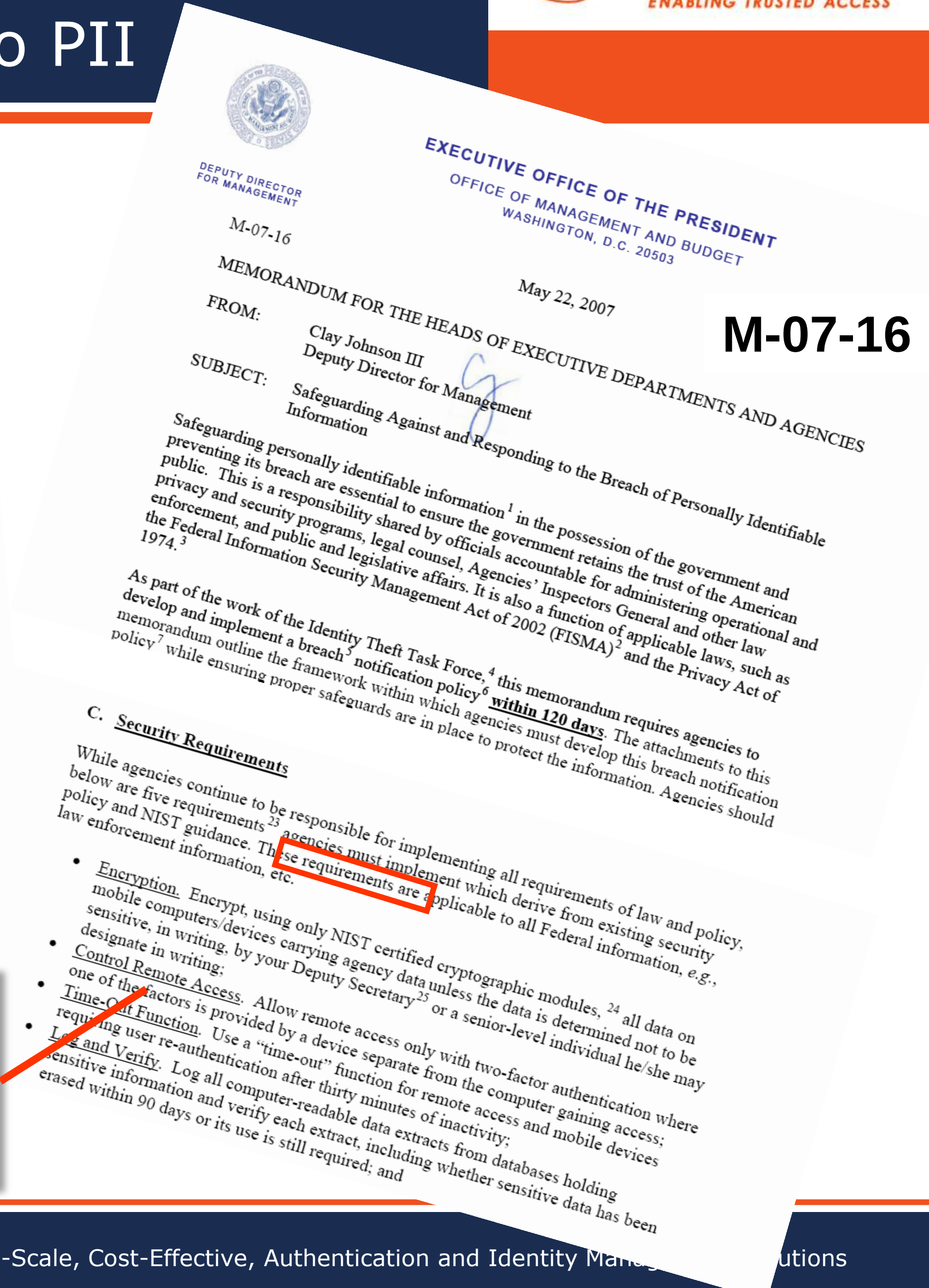
FROM: Clay Johnson III
Deputy Director for Management

SUBJECT: Protection of Sensitive Agency Information

In an effort to properly safeguard our information assets while using information technology, it is essential for all departments and agencies to know their baseline of activities.

The National Institute of Standards and Technology (NIST) provided a checklist for protection of remote information. (See attachment) The intent of implementing the checklist is to compensate for the lack of physical security controls when information is removed from, or accessed from outside the agency location. In addition to using the NIST checklist, I am recommending all departments and agencies take the following actions:

1. Encrypt all data on mobile computers/devices which carry agency data unless the data is determined to be non-sensitive, in writing, by your Deputy Secretary or an individual he/she may designate in writing;
2. Allow remote access only with two-factor authentication where one of the factors is provided by a device separate from the computer gaining access;
3. Use a "time-out" function for remote access and mobile devices requiring user re-authentication after 30 minutes inactivity; and
4. Log all computer-readable data extracts from databases holding sensitive information and verify each extract including sensitive data has been erased within 90 days or its use is still required.



M-07-16

EXECUTIVE OFFICE OF THE PRESIDENT
OFFICE OF MANAGEMENT AND BUDGET
WASHINGTON, D.C. 20503

DEPUTY DIRECTOR
FOR MANAGEMENT

M-07-16

May 22, 2007

MEMORANDUM FOR THE HEADS OF EXECUTIVE DEPARTMENTS AND AGENCIES

FROM: Clay Johnson III
Deputy Director for Management

SUBJECT: Safeguarding Against and Responding to the Breach of Personally Identifiable Information

Safeguarding personally identifiable information[1] in the possession of the government and preventing its breach are essential to ensure the government retains the trust of the American public. This is a responsibility shared by officials accountable for administering operational and privacy and security programs, legal counsel, Agencies' Inspectors General and other law enforcement, and public and legislative affairs. It is also a function of applicable laws, such as the Federal Information Security Management Act of 2002 (FISMA)[2] and the Privacy Act of 1974.[3]

As part of the work of the Identity Theft Task Force,[4] this memorandum requires agencies to develop and implement a breach[5] notification policy[6] **within 120 days**. The attachments to this memorandum outline the framework within which agencies must develop this breach notification policy[7] while ensuring proper safeguards are in place to protect the information. Agencies should

C. **Security Requirements**

While agencies continue to be responsible for implementing all requirements of law and policy, below are five requirements[23] agencies must implement which derive from existing security policy and NIST guidance. These requirements are applicable to all Federal information, e.g., law enforcement information, etc.

- Encryption. Encrypt, using only NIST certified cryptographic modules,[24] all data on mobile computers/devices carrying agency data unless the data is determined not to be sensitive, in writing, by your Deputy Secretary[25] or a senior-level individual he/she may designate in writing;
- Control Remote Access. Allow remote access only with two-factor authentication where one of the factors is provided by a device separate from the computer gaining access;
- Time-Out Function. Use a "time-out" function for remote access and mobile devices requiring user re-authentication after thirty minutes of inactivity;
- Log and Verify. Log all computer-readable data extracts from databases holding sensitive information and verify each extract, including whether sensitive data has been erased within 90 days or its use is still required; and

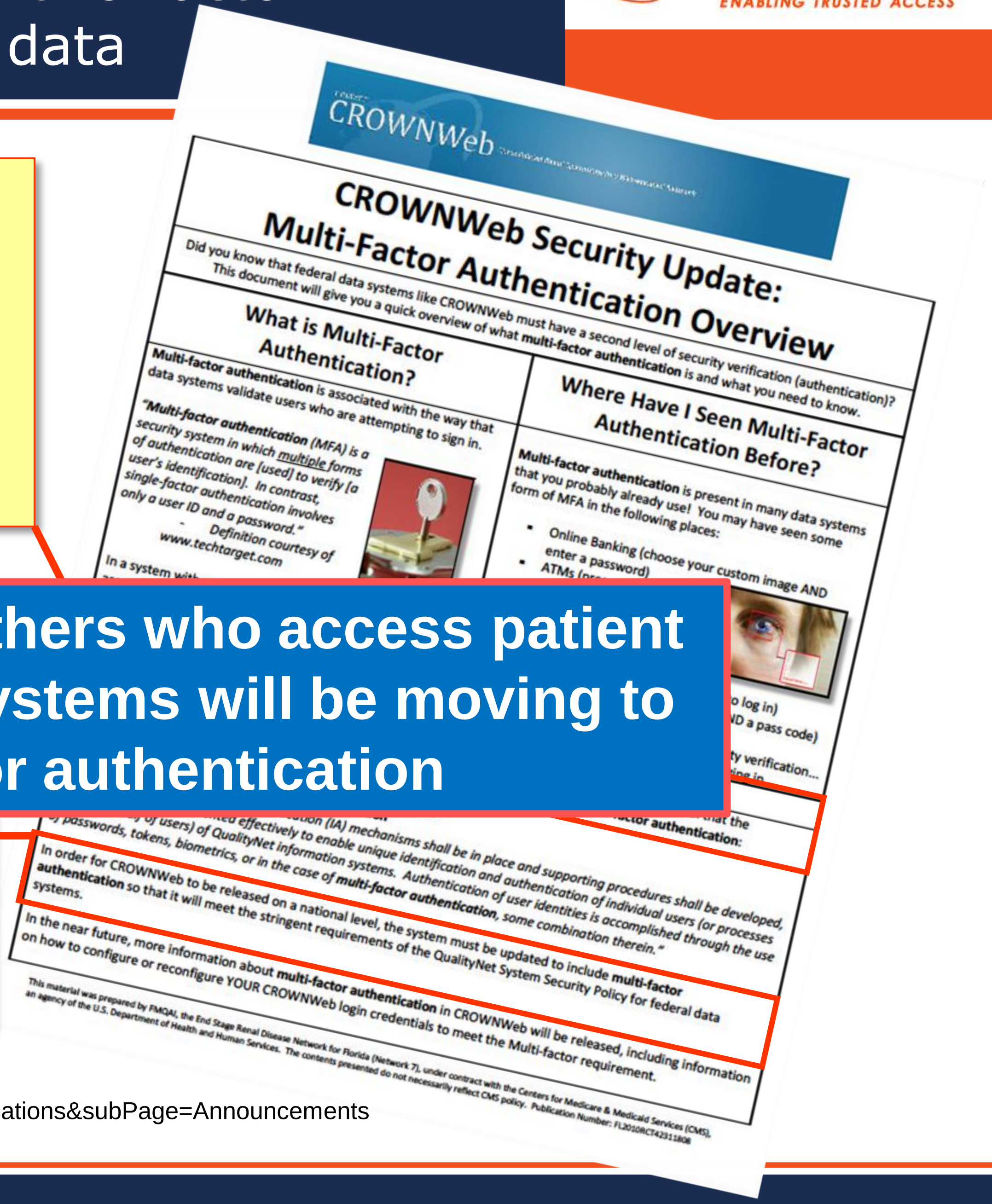
Allow remote access only with two-factor authentication where one of the factors is provided by a device separate from the computer gaining access

CMS CROWNWeb requires two-factor authentication for patient data

CROWNWeb is a federal data system which will include patient-level private health information. It is critical that the information in that system be secure. Because of this need, there is a requirement for **multi-factor authentication**

Physicians and others who access patient data on federal systems will be moving to two-factor authentication

In order fo
released o
system m
multi-facto
will meet the stringent requirements of the QualityNet System Security Policy for federal data systems.



CROWNWeb

CROWNWeb Security Update: Multi-Factor Authentication Overview

Did you know that federal data systems like CROWNWeb must have a second level of security verification (authentication)? This document will give you a quick overview of what **multi-factor authentication** is and what you need to know.

What is Multi-Factor Authentication?

Multi-factor authentication is associated with the way that data systems validate users who are attempting to sign in.

*"**Multi-factor authentication** (MFA) is a security system in which multiple forms of authentication are [used] to verify [a user's identification]. In contrast, single-factor authentication involves only a user ID and a password."*
- *Definition courtesy of www.techtarget.com*

In a system wit

Where Have I Seen Multi-Factor Authentication Before?

Multi-factor authentication is present in many data systems that you probably already use! You may have seen some form of MFA in the following places:

- Online Banking (choose your custom image AND enter a password)
- ATMs (pr
o log in)
D a pass code)
y verification...

ctor authentication:

passwords, tokens, biometrics, or in the case of **multi-factor authentication**, some combination therein."

In order for CROWNWeb to be released on a national level, the system must be updated to include **multi-factor authentication** so that it will meet the stringent requirements of the QualityNet System Security Policy for federal data systems.

In the near future, more information about **multi-factor authentication** in CROWNWeb will be released, including information on how to configure or reconfigure YOUR CROWNWeb login credentials to meet the Multi-factor requirement.

This material was prepared by FMQAI, the End Stage Renal Disease Network for Florida (Network 7), under contract with the Centers for Medicare & Medicaid Services (CMS), an agency of the U.S. Department of Health and Human Services. The contents presented do not necessarily reflect CMS policy. Publication Number: FL2010RCT42311808

http://www.projectcrownweb.org/crown/index.php?page=Communications&subPage=Announcements

CMS recommendation for strong authentication is being adopted by state HIEs

From the CA HIE Operational Plan:

Authentication- NIST Level 3 (Two-Factor)

Policy: Entities a
authentication fo
unsecured locati
may be made wi

This guidance docume
covered entity may pro
purview. In so doing.

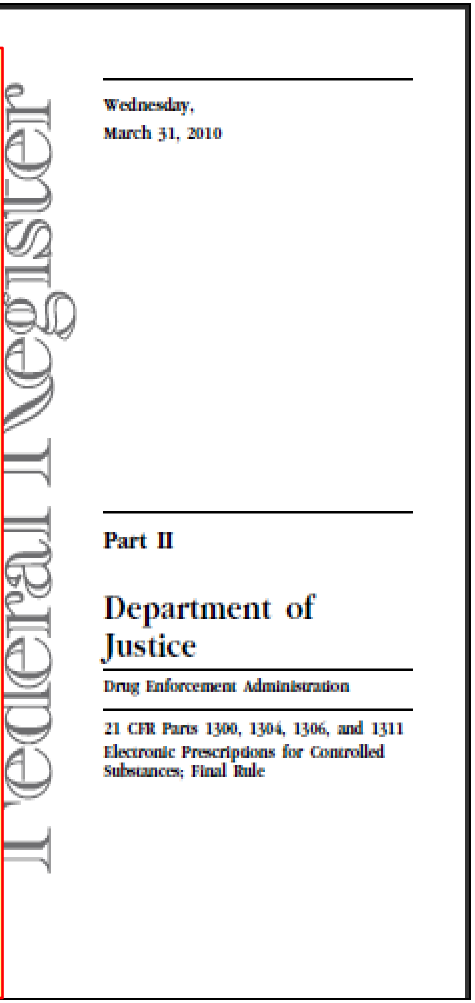
New York RHIO Authentication Standard:

- RHIOs shall be required to authenticate, or require their Participants to authenticate, each Authorized User through an authentication methodology that meets the minimum technical requirements for Level 3.
- NYeC shall …determine the implementation approach and timetable for transition to Level 3.
- Level 3 will require … RHIOs or their Participants to authenticate each Authorized User's identity using multifactor authentication, which queries Authorized Users for something they know (e.g., a password) and something they have (e.g., an ID badge or a cryptographic key).

DEA EPCS regulations require NIST Level 3 two-factor authentication

Passwords are often
described
because th
healthcare
people use
observed.
passwords
as a means
effectivene
counterpro
users to wr
which weal

DEA is requiring in this interim final rule that the authentication credential be two-factor. Two-factor authentication (two of the following—something you know, something you have, something you are) protects the practitioner from misuse of his credential by insiders as well as protecting him from external threats because the practitioner can retain control of a biometric or hard token. Authentication based only on knowledge factors is easily subverted because they can be observed, guessed, or hacked and used without the practitioner's knowledge. (p. 16242)



Federal Register

Wednesday,
March 31, 2010

Part II

Department of
Justice

Drug Enforcement Administration

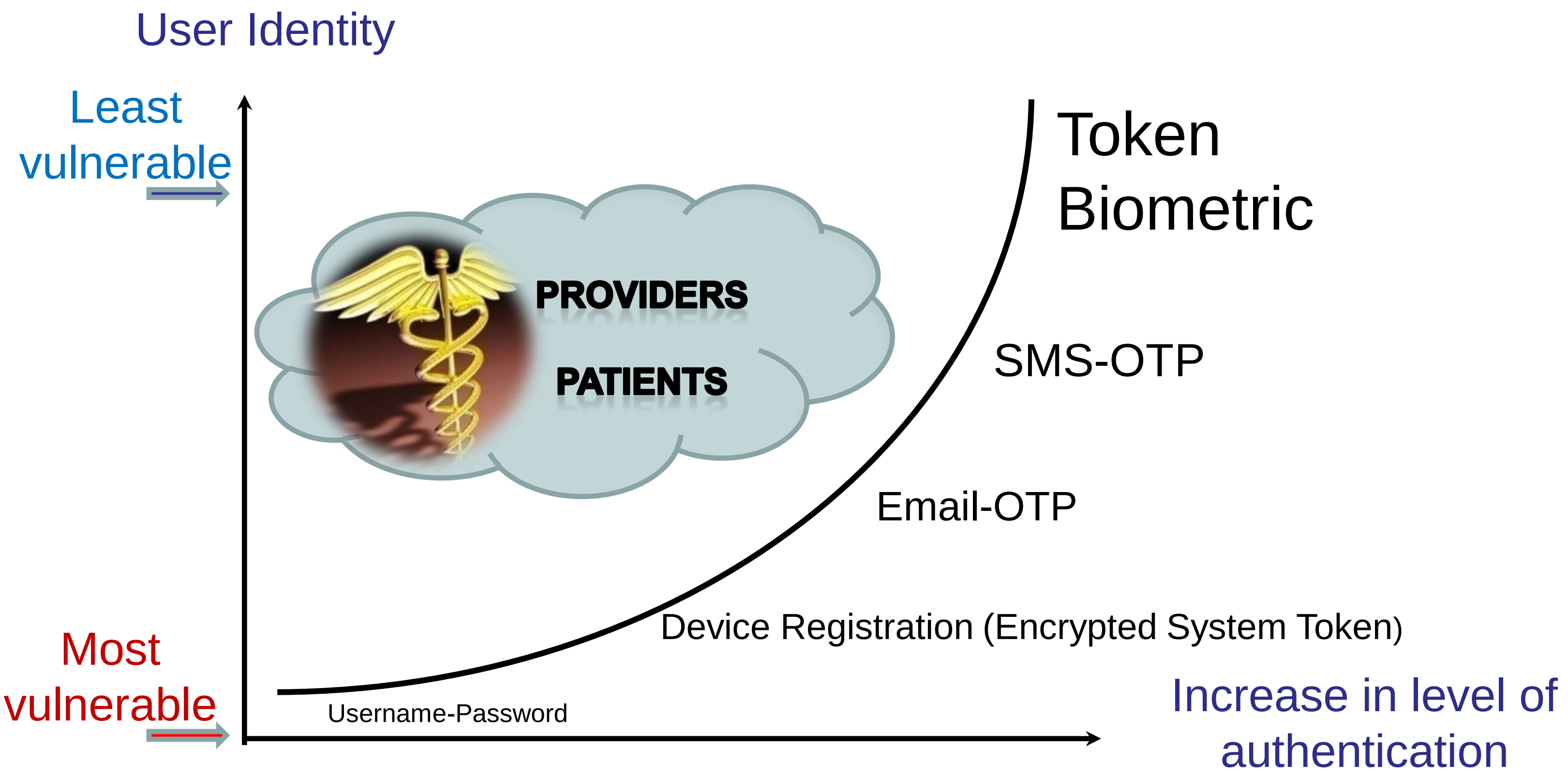
21 CFR Parts 1300, 1304, 1306, and 1311
Electronic Prescriptions for Controlled Substances; Final Rule

Traditional authentication approaches do not work well for healthcare

Current approaches to authentication do not meet the needs of a large portion of the overall identity management market

	Single Factor Authentication	Traditional Second Factor Authentication
Approach	Authenticating network and application users with a user name and password	Hard tokens, smart cards, USB devices, biometrics
Challenges	- If known by a perpetrator, he/she can easily compromise a single account or potentially an entire network - Increased complexity of password adds to password re-set costs, and users writing down passwords. - Has led to a need for second factor authentication for important/sensitive information	- Expensive to deploy and maintain ($10-$60 per user/per year) - Burdensome on the individual to carry - Prone to loss, theft, , damage, and obsolescence (non-recyclable) - Administratively cumbersome for most applications, particularly citizen-facing portals with millions of users

Vulnerability levels around authentication



User Identity

Least vulnerable

Most vulnerable

Token

Biometric

SMS-OTP

Email-OTP

Device Registration (Encrypted System Token)

Username-Password

Increase in level of authentication

- Defense against attackers who exploit weak authentication for identity theft and fraudulent transactions
- Reduction of costs derived from poor password management, identity theft, support center costs,
- Attraction of an increasing number of security-conscious consumers

Recommendations

- **Adopt stronger authentication than username/password**
  - Strength of authentication can be tailored to user role and sensitivity of system, data or application
  - Many physicians (and most likely their staff) will already be required to have second-factor credentials for e-prescribing or quality reporting to the federal government
- **Strong authentication will become more prevalent**
  - Federal systems require two-factor authentication
  - E-prescribing applications will support two-factor authentication
  - The trust fabric of the NHIN will require consistency of access control levels
  - Usability of strong authentication is improving as new technologies move to mass markets

Questions?

Anna Slomovic
aslomovic@anakam.com